1. Introduction

This Candidate Privacy Notice ("**Notice**") lets you know how we, Mauritius Network Services Ltd. (hereafter "**MNS**"), collect and use your personal data in connection with our recruiting exercise. This Notice describes the potential use of the personal data of candidates. We may however make less use of your personal data than is described here.

2. Collecting Personal Data

We may collect your personal data in connection with recruiting in the following ways:

- When you provide personal data to us directly for e.g., when you give us your Curriculum Vitae; information you provide to us via our website, emails and phone calls, interviews; and
- When you made your personal data publicly available on platforms such as LinkedIn or other job recruiting sites; and
- When your personal data is provided to us by a third party, for e.g., a recruitment agency or a previous employer or through our employee referral program.

We request certain data about you when you apply for a job at MNS, including your Curriculum Vitae, resume, educational and employment background, contact details and preferences, job qualifications, and jobs. You also may choose to provide us with additional data, such as other employment references and related data, and compensation requests.

We may collect, process, and maintain your personal data including:

Categories of personal data	Details
Contact details	First name, surname, postal address, email address, telephone/mobile number
Individual details	Gender, date of birth, age, language, photograph
Educational and professional background	CV/ resumé, academic and professional qualifications, employment history and past employers' references and/or testimonials, job skills, working conditions and study leave entitlement

National identification details	Identity card number, passport number
Financial information	Information about your current level of remuneration, including benefit entitlements, study allowances and health insurance allowances
Video surveillance	Information collected from our closed-circuit televisions ("CCTV") footage
Special categories of personal data	Certificate of character containing information about criminal convictions/allegations and offences (for vetting purposes where permissible and in accordance with applicable law and/or any information you choose to share with us such as data concerning any disability, vaccination status
Other	Information you choose to share with us such as your hobbies and social preferences

3. Special Categories of Personal Data (or "Sensitive Personal Data")

This information, when collected, is generally done so on a voluntary, consensual basis, and job candidates are not required to provide this information unless we must collect such information to comply with our legal obligations or exercise our specific rights concerning the recruitment process. For instance, you may choose to provide us with information on whether you have a disability and would like us to consider any special accommodation.

4. Voluntary Disclosure

Your provision of personal data in connection with recruiting is voluntary, and you determine the extent of data you provide to us; please note that if you decide not to provide data, it may affect our ability to consider you for employment.

5. Using Personal Data

MNS will only use your personal data for the purpose(s) for which it was collected or agreed with you. The data may be used to communicate with you, to manage our recruiting and hiring processes, and for compliance with corporate governance, legal as well as regulatory requirements. We have set out below the legal basis of processing for each purpose.

If you are hired, the data may be used in connection with your employment, performance management and corporate management as described in our Employee Privacy Notice.

We may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your personal data. Please contact the Data Protection Officer if you need details about the specific legal basis, we are relying on to process your personal data where more than one basis has been mentioned below.

Purpose of processing	Legal basis of processing
Personal data	
As required for the recruitment process at MNS: - for communicating with you, - to analyse your qualifications and references, and - to set out your job conditions.	- Consent for Reference Check - The processing is necessary to perform a contract or to take steps at your request, before entering a contract, namely your contract of employment. - For our legitimate interests namely for the proper administration of our business and to ensure appropriate job candidates are being recruited.
Storing your curriculum vitae and contact details for the purpose of contacting you for future job opportunities	- Legitimate interest
Special Categories of Personal Data	
To know whether there are previous criminal convictions recorded against you	- Legitimate interest - The processing is necessary for the purpose of carrying out our obligations and of exercising your rights

6. Access to your Personal Data

6.1. Access to your personal data within MNS

Access to your personal data is restricted to authorised personnel only (i.e., HR Dept) of MNS. Your CVs are communicated to the management team and authorised personnel for recruitment and selection purposes. All authorised personnel are required to keep your data strictly confidential.

6.2. Access to your personal data by third parties

Except as otherwise stated in this notice or as required for legal or regulatory purposes, we treat your personal data as confidential and will not disclose it to third parties without your

consent. We do not share personal data you provide to us for recruitment purposes with any other service providers or other third parties unless your employment application is successful and MNS makes you an offer of employment.

We may share your personal data with public and government authorities as required by applicable laws and regulations, for national security and/or law enforcement purposes.

7. Security and Confidentiality

We maintain reasonable administrative, physical, and technical controls designed to protect the confidentiality and security of your personal data. Our employees who may have access to your personal data are required to keep that data confidential.

We may employ security procedures at our facilities and on our computer systems to monitor and maintain security, including the use of CCTV. Any monitoring of our facilities, systems or assets is performed in accordance with applicable law.

8. Your data protection rights

Under the GDPR and the DPA, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

8.1. Your right of access to your personal data

You have the right to request a copy of the personal data we hold about you. To do this, simply contact the Data Protection Officer as per Section 13 and specify what data you would like. We will take all reasonable steps to confirm your identity before providing details of your personal data.

You will not have to pay a fee to access your personal data (or to exercise any of your other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

8.2. Your right to rectification of your personal data

You have the right to ask us to update or correct your personal data if you think it is inaccurate or incomplete. We will take all reasonable steps to confirm your identity before making changes to the personal data we may hold about you. We would appreciate it if you would

take the necessary steps to keep your personal data accurate and up-to-date by notifying us of any changes we need to be aware of. You may submit requests to correct your personal data, or any other requests concerning your personal data to the Data Protection Officer.

8.3. Your right to erasure of your personal data

You have the right to ask us to delete your personal data in certain circumstances:

- When we no longer need your personal data;
- If you initially consented to the use of your personal data, but have now withdrawn your consent;
- If you have objected to us using your personal data, and your interests outweigh ours;
- If we have collected or used your personal data unlawfully; and
- If we have a legal obligation to erase your data.

Where we collect personal data for a specific purpose, we will not keep it for longer than is necessary to fulfil that purpose, unless we have to keep it for legitimate business or legal reasons. Upon the determined expiry date, we will securely destroy your personal data as per the retention periods as indicated in Section 8.

8.4. Your right to restriction of processing

You have the right to ask us to limit how we use your data. If necessary, you may also stop us from deleting your data. To exercise your right to restriction, simply contact the Data Protection Officer as per Section 13, say what data you want restricted and state your reasons. You may request us to restrict processing of your personal data in the following circumstances:

- If you have contested the accuracy of your personal data, for a period to enable us to verify the accuracy of the data;
- If you have objected to the use of your personal data;
- If we have processed your personal data unlawfully but you do want it deleted;
- If we no longer need your personal data but you want us to keep it in order to create, exercise or defend legal claims.

8.5. Your right to object to processing

You also have the right to object to us processing your personal data where your data is being used:

- For a task carried out in the public interest;
- For our legitimate interests;
- For scientific or historical research, or statistical purposes; or
- For direct marketing.

Note that you can exercise your right to objection when we process your personal data for our legitimate interests only. However, we shall continue the processing of your personal data despite the objection raised where we have strong compelling legitimate reasons including the establishment, exercise or defence of a legal claim.

8.6. Your right to data portability

The right to data portability allows you to ask for the transfer of your personal data from one organisation to another, or to you. The right only applies if we are processing information based on your consent or performance of a contract with you, and the processing is automated. You can exercise this right with respect to the information you have given us by contacting the Data Protection Officer as per Section 13. We will ensure that your data is provided in a way that is accessible and machine-readable.

8.7. Your right to withdraw consent

To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

Note:

a) If you wish to exercise any of the rights set out above, please contact our Data Protection Officer (refer to Section 13).
b) We try to respond to all requests within one month. However, it may take us longer than a month if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

9. Retention of your personal data

Where we collect and/ or process your personal data for a specific purpose, we will not keep it for longer than is necessary to fulfil that purpose, unless we have to keep it for legitimate business or legal reasons. To the extent permitted or required by law, we may delete data at any time. Accordingly, you should retain your own copy of any data you submit to us.

If your employment application is unsuccessful, all personal data collected during the recruitment process will kept for 1 year to consider you for any future job opportunities, upon your valid consent, after which same will be deleted.

10. Your Responsibilities

You are responsible for the data you provide or make available to us, and you must ensure it is honest, truthful, accurate and not misleading in any way. You must ensure that the data provided does not contain material that is obscene, defamatory, or infringing on any rights of any third party; does not contain malicious code; and is not otherwise legally actionable. Further, if you provide any data concerning any other person, such as individuals you provide as references, you are responsible for providing any notices and obtaining any consents necessary for us to collect and use that data as described in this notice.

11. Cross Border Transfer

Your personal data may be transferred, accessed and stored globally (for example, on the cloud) as necessary for the uses and disclosures stated above in accordance with this notice. We have developed global data security practices designed to ensure that your personal data is adequately protected and where the services of a cloud service provider is used, we ensure that the service agreement entered into with the cloud service provider imposes obligations on the cloud service provider to implement security and organizational measures to protect the personal data.

Where such cross-border recipients, including our affiliates and other third parties, are found abroad, we have entered into and executed an agreement for the international transfer of personal data with them which allows for the processing of your personal data and which also incorporates provisions similar to the European Union Model Clauses requirements for transfers of personal data outside the European Union.

12. Complaints Handling

If you have any complaints regarding how we process your personal data, you should contact Data Protection Officer at dpo@mns.mu. We will review your complaint and respond as soon as reasonably practicable upon receipt of your complaint. If you are not satisfied with the way your complaint has been handled, then you can contact the Data Protection Office at dpo@govmu.org.

13. General

We may update this document from time to time to reflect best practices in data management, security and control and to ensure compliance with any changes or amendments made to the DPA and any laws or regulations thereof.

If you have any questions and concerns about this notice or its application, please contact our Data Protection Officer at dpo@mns.mu.